Volume 5, Issue 2, February 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

The Trends on Bluejacking Technology

Karthika.R, Anandhi.K

M.Sc. Computer Science- II year, Department of Computer Science,
Kanchi Mamunivar Centre For Post Graduate Studies,
Lawspet, Puducherry, India

Abstract— The mobile phone technology has developed tremendously in the past forty years since its invention in 1973 owing to its unique, wiring sans and fixation free networked system. As a communication device, the mobile devices have been gradually grown up in ways that move beyond merely providing a channel for mediated conversation. One such appropriation is bluejacking . the practice of sending short, unsolicited messages via vCard functionality to other Bluetooth-enabled phones is called Bluejacking. The Range of Bluetooth devices is very limited. It is around 10 meters for mobile phones, and about 100 meters for laptops with powerful transmitters. This technology allows mobile phone users to send business cards anonymously using Bluetooth wireless technology. Receiver does not know who has sent the message, but it has the name and model of the phone of bluejacker. This paper discusses about Bluejacking and its working process, Study of bluejacking tools and talks about its future prospects.

Keywords—Bluejacking, ethics, Bluetooth Exchange,OBEX, vCard.

I. INTRODUCTION

Bluejacking is an attack conducted on Bluetooth enabled devices like smart phones, laptops and PDAs. Bluejacking is done by an attacker termed as bluejacker or bluejack addict who forwards unsolicited messages to a user of Bluetooth-enabled device[8]. Bluejacking is the sending of unsolicited messages over Bluetooth sending a vCard which typically contains a message in the name field (i.e. for bluedating or bluechat) to another Bluetooth enabled device via the OBEX protocol. Bluetooth consist of very limited range; usually around 10 meters on mobile phones, but for laptops it can reach up to 100 meters with powerful transmitters [6]. Bluetooth is for synchronizing email, sending messages, or connecting to a remote headset. This message-transmitting attack resembles spam and phishing attacks conducted against email users.Bluejacking can be perceived as either infuriating or amusing, though it is relatively risk-free since the recipient has the option to decline. To choose the recipients of bluejacks, the senders complete a scan using their mobile phones to search for the available Bluetooth-enabled devices in their in and around area.[3] A bluejacker picks one of the Bluetooth enabled available devices and composes a message within a body of the phone's contact interface and sends the message to the recipient, and remains in the vicinity to observe any reactions expressed by the recipient. Bluejacking sure makes for an interesting wake-up call in close-knit environments like underground metro trains, buses, malls and cinemas.[1]

II. ORIGIN

This bluejack concept started after a Malaysian IT consultant named "Ajack" posted a comment on a mobile phone forum. The Ajack told to IT Web that he used his Ericsson mobile phone in a bank to send a short message to someone with a Nokia 7650. He got bored while standing in a bank queue, so Ajack did a Bluetooth discovery to see if there was another Bluetooth device in and around. He discovered a Nokia 7650 in the vicinity, So he created a new contact and filled the first name with,"Buy Ericsson!" and he sent a business card to that Nokia 7650 phone.[6] Thus Bluejacking has become very popular among most of the young people wanting to play some practical jokes. A 13-year-old boy named Ellie from Surrey in the UK has started a dedicated bluejacking site called bluejackq.

III. BLUEJACKING TECHNOLOGY

The Bluetooth port of the mobile phones is subject to threat of bluejacking attacks. Bluejacker carefully crafts the identification that devices exchange during association and then transmits a short unsolicited text messages into authentication dialogs. Thus, bluejacker tricks the user and gains access to user's phone book, Photos, or files which residing on the device. Bluejacking is base on following technologies[1]

A. Bluetooth Technology:

Bluetooth Technology was developed to solve the simple problem of eliminating the data cable. The idea is to replace the data cables that are needed to accompany portable devices which are carried out by many mobile travelers along with a less-cost, more secure and robust RF link. Originally Bluetooth were marketed to small handheld devices such as mobile phones and laptops. As the Bluetooth standard emerged and developed successfully into society, the

world demanded more Bluetooth and so its very efficient, effective, and secure that even the IEEE approved the 802.15.1 Standard for Wireless Person Area Networks (WPAN) based on the Bluetooth specification.[6]

1. Bluetooth as Cable Replacement Technology:

Bluetooth is competent of transmitting voice, data, video clips and pictures. It can be used to wirelessly synchronize and transfer data among many devices and can be thought of as a data cable replacement technology [1].

2. Future Trends in Bluetooth Technology:

The Bluetooth Interest Group is an industry group consisting of leaders in the telecommunications, computing, and networking industries that are driving development of the technology and bringing it to market [1].

B. Obex Protocol:

Here OBEX (stands for OBjectEXchange, also termed as IrOBEX) is a one of the communications protocol that facilitates the exchange of binary objects between devices. It is been adopted by the Bluetooth Special Interest Group and the SyncML wing of the Open Mobile Alliance(OMA) and it is maintained by the Infrared Data Association . Palm III personal digital assistant is the one of OBEX's earliest popular applications [10].

***1. OBEX as the heart of Bluetooth file transfer*:**

Object Exchange, or OBEX protocol is the heart of file transfer over Bluetooth. A binary file transfer protocol run over not merely Bluetooth but also infrared and even generic TCP/IP. http://openobex.sf.net it offers the most ubiquitous open source implementations of the protocol [1].

2. OBEX connection overview:

(i) CONNECT: Here it one of the fields that specifies the largest size of packets the client can receive and the servers answer with its maximal packet length, and its connection id, and other data.
(ii) GET: Here the client requests a file, and it specifying the connection id, the file name and/or its type; and then the server answer with the file content.
(iii) SETPATH: Here the client tells the server to switch to a different file folder, and its specifying the connection id and the folder name in two headers.
GET: Here the client request a listing of the folder content by sending an object with the connection id.
(iv) PUT: Here the client sends a file to the server; if file is too large to fit into a one/single packet, then the server will request to the next part with a CONTINUE response
(vi) DISCONNECT: Here the client informs the server that is closing the session [10].

3. Protocols runs over OBEX:

The following are some of protocols runs over OBEX:
(i) OBEX File Transfer Protocol: It is used to store and retrieve where OBEX Push: It is used for transferring a file from the originator of the request to the recipient.
(ii) Files are similar to FTP
(iii) Phonebook Access: It is similar to file transfer, but uses a phonebook entries can be listed (with various possible orderings and filters) and retrieved from certain directories under telecom/ using GET and SETPATH[10].

***4. Devices supported by OBEX*:**

(i) Devices are most sharp, motorola, samsung, sony ericsson, HTC and nokia phones with infrared or Bluetooth port. These all are supported by OBEX
(ii) Users LG EnV Touch (VX11000).
(iii) And many other PDAs since 2004[1].

C. vCard Functionality:

1. vCard Features:

(i) vCards are similar like a structured blocks of text data that provide the content what is more or less an electronic business card. Here the data can be name, address, telephone numbers (no may be of home, business, fax, pager, cellular, ISDN, voice, data, video), and e-mail ID and related internet URLs.
(ii) vCards can also contain graphics and multimedia, that includes photographs, company logos, audio clips, along with the geographic and time-zone informations.
(iii) vCards can also designed to support multiple languages ,transport and the operating system independent[11].

2. Applications of vCards:

(i) Infrared Exchange
(ii) Bluetooth Exchange.
(iii) Internet Mail
(iv) Computer/Telephony Applications
(v) Video and data conferencing[1]

IV. HOW TO BLUEJACK

First Assume that you now have a Bluetooth phone in your hands, the thing is to make sure that Bluetooth is enabled. Then you will need to read the handbook of the particular phone (or PDA etc) that you have but somewhere in the Menu item then you will find the item that may enables and disabled Bluetooth.

Steps are as follows:

(i) Bluetooth devices only work over short distances, so we need to find a big crowd. Bluejacking is a very new technology so not everyone will have a Bluetooth phone or PDA. So the bigger the crowd the more we may find a 'victim'.

(ii) We now need to create a new Contact in our Phone Book - rather putting someone's name in the Name field we must write short message like - "Hey, you have been BlueJacked!"[6] .

(iii) Press done/ok option. Save this new contact in the phone/address book of mobile phone/laptop respectively.

(iv) Then click on the contact created. Go to action. choose "via Bluetooth" or "Send to Bluetooth" option.

(v) Click the "Search" option for discovering active Bluetooth devices. Select a device from those list.

(v) After the selection of the particular device, the short message would be transmitted to it. Thus, the device Would be bluejacked[2].

Fig. 2 How sender sends the bluejack message [12]

Fig. 3 What does receiver sees on the screen as it receives the bluejack message [12]

V. STUDY ON BLUEJACKING TOOLS

The procedure for bluejacking as stated or explained earlier are very long and confusing. To avoid this confusion we have developed some software to do bluejacking activities in an easier way. So by downloading that software on our personal computer or on your Bluetooth configured or enabled mobile phone we can do it directly by just searching the Bluetooth enabled device and send an unsolicited messages. There are many software tools available in the market and the name is according to their usage. Some of tools are as follows:

(i) *RedFang:* Whitehouse has designed a software tool called RedFang which can discover a Bluetooth enabled devices that have been set to be non discoverable.

(ii) *Bluesniff:* BlueSniff is a simple utility for finding discoverable and hidden Bluetooth-enabled devices. It operates on Linux and it is a graphics tool, [7].

(iii) *Bluescanner:* Blue Scanner searches out for *the* Bluetooth-enabled devices and try to extract as much information as possible for each newly discovered device in other words one can use this one to spy on others who are close[8].

(iv) *Bluesnarfing:* Bluesnarfing is a method of hacking into Bluetooth-enabled mobile phone and with this we can

copy its entire information like contactbook, pictures, their data etc. With this software we give the complete freedom to hacker, to send a "corruption code" which will completely shut-down the phone down and make the phone unusable. [9]

(v) *Bluebugger:* This simply exploits the BlueBug (It's the name of some set of Bluetooth security holes) vulnerability of the bluetooth-enabled devices. By exploiting this one can access phone-books, calls lists, data and other information of that device.

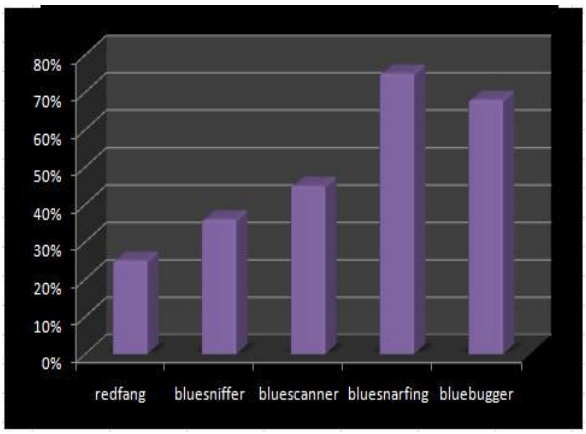

Fig. 4 Statistical report on bluejacking tools

VI. CONCLUSION

Bluetooth is a greatest technology with so many useful application. At the meanwhile, variety of Bluetooth hacking tools and techniques are available in this world, Bluejacking being the most vulnerable , which makes a lot and it claims a little riskier to use this technology. And looking at its current use and misuse also by few people, it is expected that in the future, it may have the following aspects that is either it will be used extensively and people would be able to get all the necessary information on their devices if they have their Bluetooth on. Else people will stop using Bluetooth even and only bluejackers will be playing with each other for fun. Bluetooth is not going to go away because of a few security flaws; instead it can be secure if configured properly and used carefully with a proper understanding of this wonderful technology. So, use this technology properly as it is intended and get best of it, rather than just making wrong use of it and irritating others. And Users need to be made aware of the vulnerabilities of these devices so that it employ user in more effectively, confidently and safely.

ACKNOWLEDGMENT

The author is greatly obliged to thank college management for their Collaboration in developing this paper. The author wishes to thank department professors for their valuable guidance and encouragement. And also the author sincerely thank and acknowledge all authors for their contributions and research findings directly and indirectly which used in this paper.

REFERENCES

[1] (IJETT) – Volume 4 Issue 7- July 2013 ISSN: 2231-5381 http://www.ijettjournal.org Page 3020 Bluejacking Technology: Overview, Key Challenges and Initial Research.
[2] www.ijecs.in-the new and clear approach to bluejacking.
[3] Bluetooth_hacking_browning_kessler-a case study
[4] Bluejacking-slideshare.
[5] A RAINIER PR WHITE PAPER Bluejacking as a Marketing Channel.
[6] http://seminarprojecttopics.blogspot.in
[7] From Bluetooth to RedFang-By Peter Piazza
[8] Bluetooth Security & Vulnerabilities information security management handbook
[9] http://www.bluejackq.com/bluetooth special interest group
[10] http://en.wikipedia.org/wiki/obex
[11] http://en.wikipedia.org/wiki/vcard functionality
[12] http://en.wikipedia.org/wiki/Bluejacking

